UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/871,672	06/04/2001	Prakash Panjwani	06944.0036	2391

293 7590 09/22/2004

DOWELL & DOWELL PC
2111 Eisenhower Ave.
Suite 406
Alexandria, VA 22314

EXAMINER	
NGUYEN, MINH DIEU T	
ART UNIT	**PAPER NUMBER**
2137	10

DATE MAILED: 09/22/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/871,672	PANJWANI ET AL.	
	Examiner	Art Unit	
	Minh Dieu Nguyen	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 June 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *7-48* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *7-20,22, 25, 27-35, 37-46,48* is/are rejected.

7)☒ Claim(s) *21,23,24,26,36 and 47* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 6.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. The preliminary amendment dated June 4, 2001 has been entered with the cancellation of claims 1-6 and the addition of claims 7-48.

Claims 7-48 are pending.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claim 23 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The phrase "the two MACs" lacks antecedent basis as claim 7, step (e) only states first MAC.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. **Claims 7-16, 22, 27-31, 38-42 and 48** are rejected under 35 U.S.C. 103(a) as being unpatentable over Reeds, III et al. (5,153,919) in view of Diffie et al. (Re. 36,946) and further in view of Chen et al., (5,784,463).

a) **As to claims 7, 27, 38 and 48**, Reeds discloses an authenticating protocol for insuring validity of communicating radio-telephones which has mobile telephone with its identity (col. 4, lines 30-34), cellular radio providers with each having one or more base stations (Fig. 1) and each mobile has it own pair of RSA keys (private and public keys) (col. 2, lines 30-31), the method comprising "secret" A-key, assigned to customer's mobile telephone by service provider (col. 4, lines 37-39; lines 43-45), the A-key is used to create shared secret data (SSDs) (Fig. 4) and these SSDs are used to support authentication procedures (Fig. 2) and generating session keys for encrypting signaling messages (col. 6, lines 12-16; Fig. 8), it largely anticipates limitations of steps d-e) and steps g-l) except Reeds' invention does not disclose base station identity which MAC is computed on.

Diffie discloses a system using both public key and shared key encryption techniques for communications between wireless mobile devices and a base station (col. 5, lines 33-37) comprising each participant generates a public/private key pair (col. 5, lines 59-63), base station sends a message to mobile device with its identity (col. 6, lines 2-5; col. 8, lines 7-22) which anticipates steps a-b).

Reeds discloses shared secret data is generated from the A-key, however he and Diffie do not disclose the steps of generating a pair of secret keys as described in steps c and f.

Chen discloses a system and method for generating a shared secret key being based on a public/private key (col. 3, lines 13-24) reading on steps c and f. Chen also discloses the shared secret key can be used for mutual authentication, which reads on first pair of secret key for authentication in steps d-e) and steps g-j), and development of session keys to secure subsequent communications (Abstract) which reads on steps k-l). Chen does not disclose the session key is computed from the second pair of secret keys and short-lived public key and the random challenge.

The examiner takes official notice that use of random challenge for providing different keys as needed in performing session key and the use of another parameter as short-lived public key in computing session key so as intruder has one more parameter to go after if other parameters in the session key get compromised are quite well known in the data encryption art.

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of base station's identity, its public/private key and generation of shared secret key based on combination of public/private key of each entity in the system of Reeds, as Diffie and Chen teach, so as to provide sufficient security services.

b) **As to claim 8**, Reeds discloses the first correspondent is a mobile station and the second correspondent is a base station (Fig. 1, elements 22, 23, 30-40).

c) **As to claims 9-10**, Reeds discloses the secure communication is a call originated by the mobile station (col. 1,lines 21-24) and call terminating at the mobile station (col. 3, lines 40-45).

d) **As to claims 11 and 13**, Reeds discloses the secure communication is data exchange between the stations and data exchange is used for financial transactions (Fig. 8; col. 10, lines 8-21).

e) **As to claim 12**, Chen discloses data exchange is used for internet browsing (col. 2, lines 10-12).

f) **As to claims 14, 28 and 39**, Reeds discloses the service provider could supply each mobile with its own pair of private and public keys (col. 2, lines 30-31), the second correspondent obtains the public key from a service provider of the first correspondent (col. 3, lines 8-23; col. 8, lines 5-6).

g) **As to claims 15-16, 30-31 and 41-42**, Diffie discloses the public key is transmitted to the service provider by a manual exchange using a dial-up connection (col. 5, lines 61-63). Diffie does not disclose dial-up connection, however it is quite know

in data communications art. It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of dial-up connection so as to provide variety of means to exchange public key.

h) **As to claims 22, 29 and 40**, Reeds discloses the second correspondent is a service provider of the first correspondent (Fig. 1).

6. **Claims 17-18, 32-33 and 43-44** are rejected under 35 U.S.C. 103(a) as being unpatentable over Reeds, III et al. (5,153,919), in view of Diffie et al. (Re. 36,946), further in view of Chen et al., (5,784,463) and further in view of Maruyama et al. (5,883,960).

Reeds discloses the ESN number is installed in the mobile unit by the manufacturer at the time the unit is built, however Reeds, Diffie and Chen do not disclose the service provider obtains the public key by an exchange at manufacture time.

Maruyama discloses the mobile unit public keys are written during the manufacture of the mobile units (col. 9, lines 15-19).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use exchanging public key at manufacture time so as to provide variety of means to exchange public key.

7. **Claims 19-20, 34-35 and 45-46** are rejected under 35 U.S.C. 103(a) as being unpatentable over Reeds, III et al. (5,153,919), in view of Diffie et al. (Re. 36,946), further in view of Chen et al., (5,784,463) and further in view of Quick, Jr. (6,260,147).

Reeds, Diffie and Chen do not disclose service provider obtains public key by an over-the air exchange and the exchange is secured using a password.

Quick discloses the service provider obtains public key by an over-the air exchange and the exchange is secured using a password (Fig. 1; col. 2, lines 30-47).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use exchanging public key over the air exchange so as to provide variety of means to exchange public key.

8. **Claims 25 and 37** are rejected under 35 U.S.C. 103(a) as being unpatentable over Reeds, III et al. (5,153,919), in view of Diffie et al. (Re. 36,946), further in view of Chen et al., (5,784,463) and further in view of Venkatesan et al. (6,209,093).

Reeds, Diffie and Chen do not disclose using elliptic curve to compute the private keys, public keys and MACs.

Venkatesan discloses the private, public keys and MACs are computed using elliptic curve cryptography (col. 10, lines 33-53).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of elliptic curve cryptography to compute public, private keys and MACs in the system of Reeds, Diffie and Chen, as Venkatesan teaches so as to make the system more efficient.

Allowable Subject Matter

9. Claim 21, 24, 26, 36 and 47 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

10. Claim 23 would be allowable if rewritten to overcome the rejection(s) under 35 U.S.C. 112, second paragraph, set forth in this Office action and to include all of the limitations of the base claim and any intervening claims.

Conclusion

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dieu Nguyen whose telephone number is 703-305-9727. The examiner can normally be reached on M-F 6:00-2:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on 703-306-3036. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Minh Dieu Nguyen
Examiner
Art Unit 2137

mdn
9/13/04

Andrew Caldwell
Andrew Caldwell